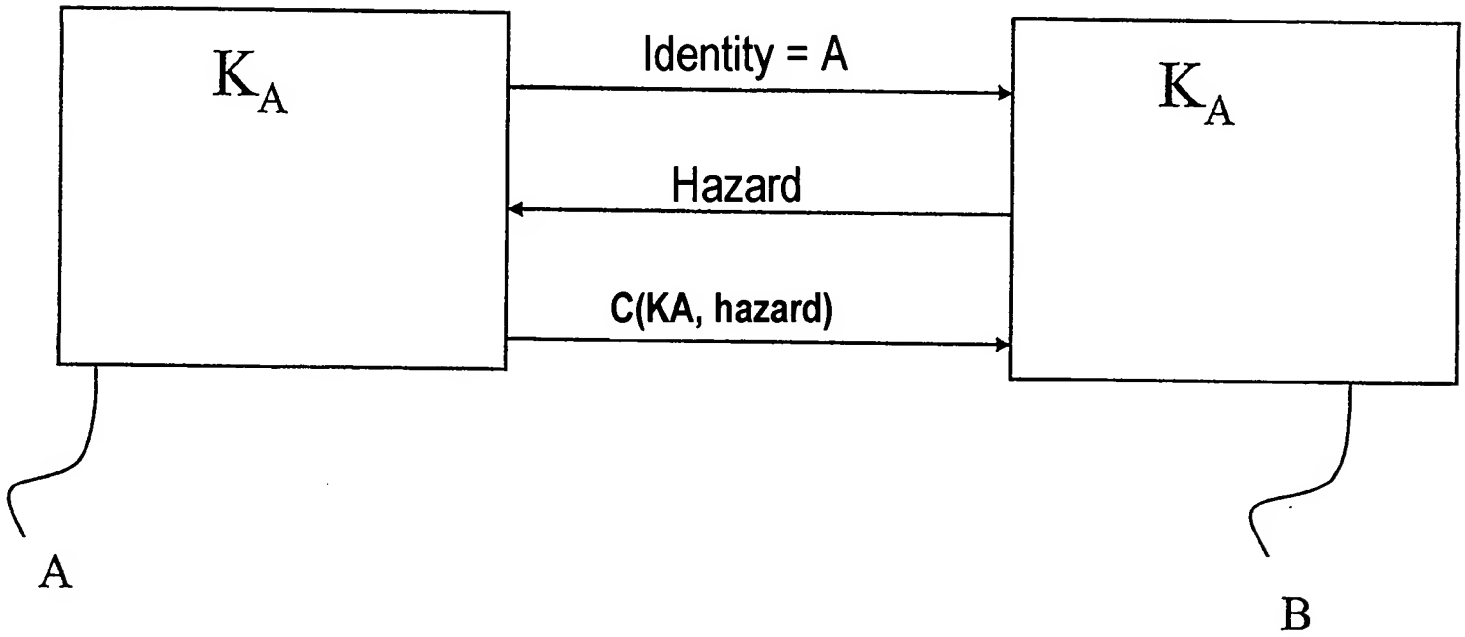


**Fig.1**
**(prior art)**

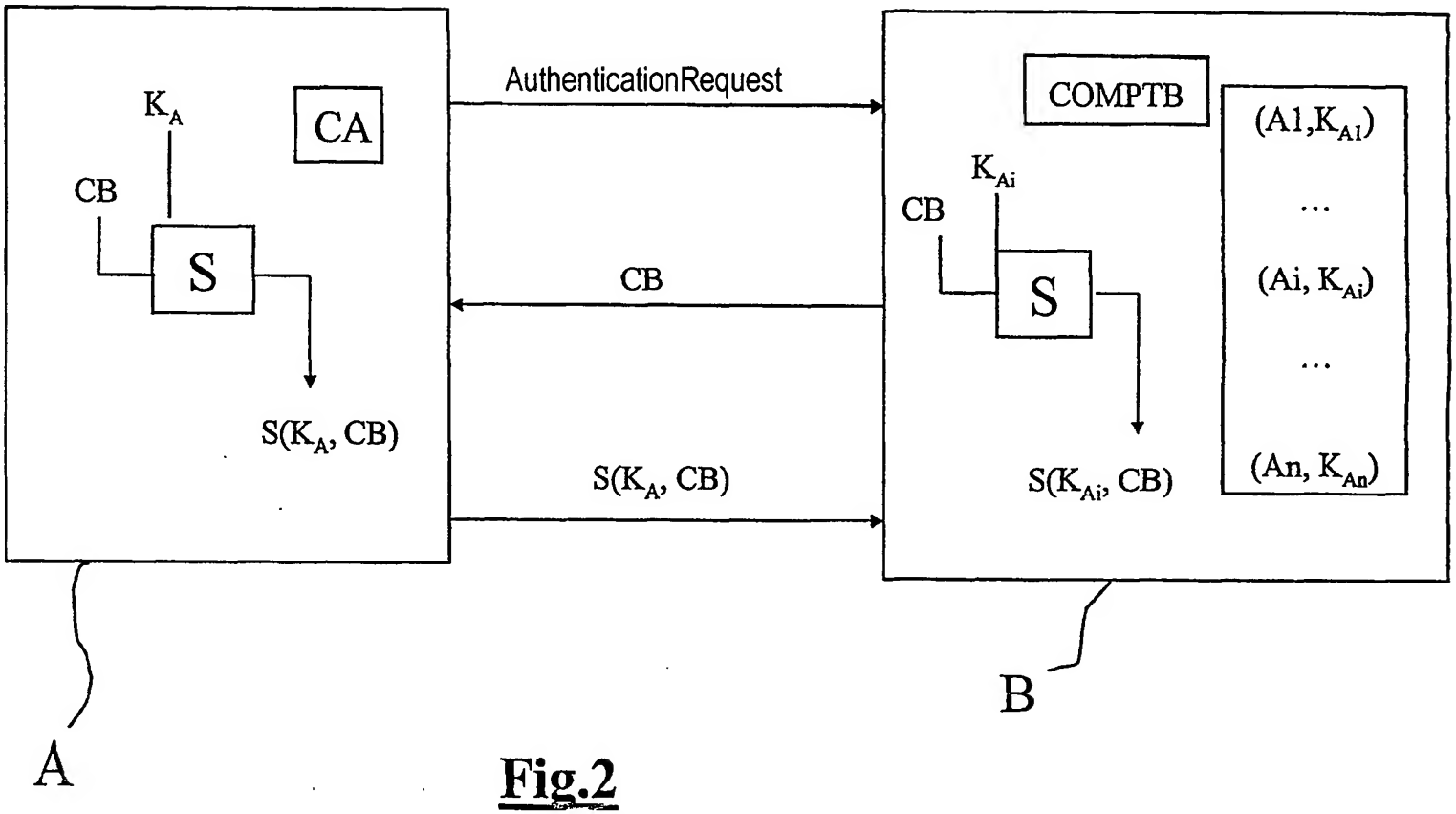
$K_A$
CA
CB
S
$S(K_A, CB)$
AuthenticationRequest
CB
$S(K_A, CB)$
COMPTB
$K_{Ai}$
CB
S
$S(K_{Ai}, CB)$
$(A1,K_{A1})$
...
$(Ai, K_{Ai})$
...
$(An, K_{An})$
A
B

**Fig.2**